Method and System for Securely Timestamping Digital Data

Field of the Invention

[001] The invention relates generally to timestamping of digital data, and in particular to a method and system for securely timestamping of digital data.

Background of the Invention

[002] The Internet is one of the fastest growing and ubiquitous modes of commerce. Many companies have Internet servers prepared for commercial delivery of goods and services. At first, the products found on the Internet or more specifically, the world wide web (WWW) were computer-based products, but today, more and more businesses are competing to set up commercial services on the world wide web.

[003] In many situations there is a need to establish the date on which a document was created and to prove that the text of a document in question is in fact the same as that of the original dated document. A traditional solution to this problem is to use a notary public. Traditional notarization is time-consuming, requires the physical presence of a licensed notary, does not detect many kinds of document tampering, and provides security relying solely on the integrity of the notary.

[004] The increasingly widespread use of electronic documents, which include digital representations of readable text but also of video, audio, and pictorial data, now poses a serious challenge for establishing the date of any such document. Furthermore, the authentication of documents in a digital data format is achieving a greater significance in that it is becoming relatively common to exchange digital documents between parties to a transaction. For example, using Electronic Document Interchange (EDI) many companies now exchange purchase orders, invoices or similar documents electronically. However, if a dispute arises as to what was transmitted as opposed to what was received it is difficult to establish which version of a document is correct and/or has precedence in time. As a result, many EDI transactions having any monetary significance are normally confirmed with physical documents to provide a paper

audit trail. However, reducing documents to physical form defeats in large measure the advantages of EDI.

[005] Techniques for timestamping documents in digital data format are known in the art. For example, techniques for timestamping documents in digital data format are disclosed in US Patent 6,188,766 issued to Kocher February 13, 2001, US Patent 5,136,647 issued to Haber et al. August 4, 1992, US Patent 5,022,080 issued to Durst et al. June 4, 1991 and US Patent 5,001,752 issued to Fischer March 19, 1991, which are incorporated hereby for reference. All these techniques are based on the steps of providing a document, hashing the document, providing time data and encrypting the hashed document with the time data using an encryption key of a timestamping module. When the encrypted data is decrypted it verifies the timestamp as accurate.

[006] However, these techniques are prone to tampering during test of a timestamp module or before a key is designated for timestamping purposes only. For example, if there is a secure key for use in encryption stored within a module false time data could be passed along with a document. The document is hashed and the time data and the document are encrypted with the key. The result looks like a timestamp. If that key later becomes a timestamping key or is set to timestamping by a dishonest person tampering with the module there is no guarantee that a timestamp is authentic.

[007] Therefore, in an attempt to overcome these security risks of the prior art, it is an object of the invention to provide a method for secure timestamping of digital data.

[008] It is further an object of the invention to provide a method and system for securely timestamping digital data.

Summary of the Invention

[009] In accordance with the present invention there is provided a method for securing timestamping of digital data comprising the steps of:

providing a secure encryption key;

providing a processor for performing security functions with the secure encryption key, the processor operable in a first mode wherein the secure encryption key is used for encryption operations and in a second mode in which the secure encryption key is only used for timestamping operations,

wherein once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions in the first mode with the secure encryption key;

receiving a request to perform a timestamping operation;

placing the processor in the second mode of operation once the request is received;

generating a unique code for being embedded within timestamped digital data, the unique code being indeterminable before receipt of the request; and,

inserting the unique code within each timestamped digital data.

[0010] In accordance with the present invention there is further provided a method for securely timestamping digital data comprising the steps of:

providing a secure encryption key;

providing a processor for performing security functions with the secure encryption key, the processor operable in a first mode wherein the secure encryption key is used for encryption operations and for test operations and in a second mode in which the secure encryption key is only used for timestamping operations, wherein once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions in the first mode with the secure encryption key;

when the processor is in the first mode of operation, receiving a first request to perform a timestamping operation on first digital data and then placing the processor in the second mode of operation; and

generating a unique code for being embedded within timestamped digital data, the unique code being indeterminable before receipt of the first request.

[0011] In accordance with the present invention there is further provided a method for securely timestamping digital data comprising the steps of:

receiving from a real time clock data indicative of a real time the first request for a timestamping operation has been received;

generating a first timestamp based on the data indicative of real time using the secure encryption key;

embedding the first timestamp within the first digital data and inserting the unique code within the first digital data; and

encoding the first digital data with inserted data therein to form timestamped digital data.

[0012] In accordance with the present invention there is further provided a receiving a second request to perform a timestamping operation on second digital data;

receiving from the real time clock data indicative of a real time the second request for a timestamping operation has been received;

generating a second timestamp based on the data indicative of a real time using the secure encryption key;

embedding the second timestamp within the second digital data and inserting the unique code within the second digital data; and

encoding the second digital data with inserted data therein to form timestamped digital data.

[0013] In accordance with an aspect of the present invention there is provided a method for securely timestamping digital data comprising the steps of:

receiving securely timestamped digital data, wherein the securely timestamped digital data have a unique code embedded therein, and wherein the unique code has been generated by a processor after the processor has been placed in a mode of operation in which a secure encryption key is only used for timestamping operations;

decrypting the timestamp using a key corresponding to the secure encryption key for providing time data in dependence thereupon;

retrieving the unique code from the securely timestamped digital data; and,

comparing the unique code with reference data in order to produce a comparison result, and if the comparison result is indicative of a match indicating authenticity of the time data.

[0014] In accordance with another aspect of the present invention there is provided a secure system for securely timestamping digital data comprising:

at least a first port for receiving the digital data and for providing timestamped digital data; and

a processor for:

performing security functions with the secure encryption key, the processor operable in a first mode wherein a secure encryption key is used for encryption operations and for test operations and in a second mode in which the secure encryption key is only used for timestamping operations, wherein once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions with the secure encryption key in the first mode; and,

for inserting in the second mode a unique code for being embedded within the timestamped digital data, the unique code being indeterminable outside the system before the processor is placed in the second mode, within the timestamped digital data.

Brief Description of Figures

[0015] Exemplary embodiments of the invention will now be described in conjunction with the following drawings, in which:

[0016] Figure 1is a simplified flow diagram of a the method for securing timestamping of digital data according to the invention;

[0017] Figure 2a is a simplified flow diagram of a method for securely timestamping digital data according to the invention;

[0018] Figure 2b is a simplified flow diagram of a method for securely timestamping digital data according to the invention;

[0019] Figure 2c is a simplified flow diagram of a method for securely timestamping digital data according to the invention;

[0020] Figure 3a is a simplified flow diagram of another method for securely timestamping digital data according to the invention;

[0021] Figure 3b is a simplified flow diagram of another method for securely timestamping digital data according to the invention;

[0022] Figure 3c is a simplified flow diagram of an embodiment of the method for securely timestamping digital data according to the invention illustrated in Fig. 3b;

[0023] Figure 4 is a simplified flow diagram of a method for securely timestamping digital data according to the invention; and,

[0024] Figure 5 is a simplified block diagram of a system for securely timestamping digital data according to the invention.

Detailed Description of Preferred Embodiments

[0025] Prior art timestamping techniques are based on the steps of providing a document, hashing the document, providing time data and encrypting the hashed document with the time data using an encryption key of a timestamping module. When the encrypted data is decrypted it verifies the timestamp as accurate. However, these techniques are prone to tampering. For example, a dishonest person provides a document together with false time data for encryption using the encryption key of the timestamping module. The document is hashed and the time data and the document are encrypted with the key. If a recipient decrypts these data it appears as a valid timestamp using the secure key of the module. Furthermore, if that key is later used for timestamping, there is no guarantee that a timestamp is authentic.

[0026] The drawbacks of the prior art as described above are overcome by the method for securing timestamping of digital data according to the invention illustrated in Fig. 1. In the following disclosure the expression "digital data" refers to any type of document available as an electronic file for processing using a digital processor. Such electronic files are, for example, readable text files, audio files, video files, picture data files, electronic data, database entries, transaction records, system records, etc. A secure encryption key is provided within a timestamping module. The timestamping module comprises a processor for performing security functions with the secure encryption key. The processor is operable in a first mode wherein the secure encryption key is used for encryption operations and for test operations and in a second mode in which the secure encryption key is only used for timestamping operations. In order to secure the timestamping the processor is precluded from performing further functions in the first mode with a secure encryption key once the processor performs a function with the same secure

encryption key in the second mode. For instance, when the processor receives a request to perform a timestamping operation using a first key, the processor places itself in the second mode of operation with respect to the first key precluding the processor from performing further functions in the first mode with the first key.

[0027] This provides secure timestamping. Since the first timestamp operation time is known, it is impossible to falsify timestamps by encrypting digital data with time data dated backward in time. All timestamps indicate a time being equal or later than the time instance when the processor has been placed in the second mode of operation with respect to the first key. Therefore, timestamps indicating a time before the time instance when the processor has been placed in the second mode of operation with respect to the first key and using the same first key are false. This allows verification of authenticity of a timestamp by comparing the time indicated by the timestamp with the time instance the processor has been placed in the second mode with respect to the key used to create the timestamp.

[0028] However, it is still possible to falsify timestamps by encrypting digital data with time data dated forward in time.

[0029] In order to render also this possibility futile an exemplary method for securing timestamping of digital data according to the invention comprises the additional step of generating a unique code associated with the first key for being embedded within timestamped digital data. This unique code is indeterminable outside the timestamping module before receipt of the request to perform a timestamping operation, i.e. before the processor is placed in the second mode of operation with respect to the timestamping key. The unique code is then inserted within each timestamped digital data. For example, each timestamped digital data comprises a timestamp having the unique code inserted within the timestamp. This method allows the authenticity of a timestamp to be verified by verifying the timestamp for authenticity and by verifying the unique code associated with the key used for performing the timestamp operation. Since the unique code is only published once the processor is within the second mode of operation with respect to the timestamping key, there is no way to create a timestamp with the unique number before it is published other than a brute force approach – timestamping every

possible unique number. Of course, selection of a sufficiently large unique code or some other form of unique code will prevent brute force attacks from being effective. Preferably, the unique code is sufficiently large to dissuade brute force attacks.

[0030] Further preferably, the secure encryption key and the processor are provided within a secure module and the unique code is indeterminable outside the module prior to receipt of the request to perform a timestamping operation.

[0031] As is obvious to persons of skill in the art, there are numerous ways to generate a unique code. Examples for generating the unique code include generating the unique code based on the secure encryption key, generating the unique code based on a random number, and generating the unique code based on a real time indicative of a time instance a first request to perform a timestamping operation has been received or a combination.

[0032] Referring to Figs. 2a - 2c, simplified flow diagrams of a method for securely timestamping digital data according to the invention are illustrated. Here the above method for securing timestamping of digital data according to the invention is applied to provide secure timestamping operations. A secure encryption key is provided within a timestamping module. The timestamping module comprises a processor for performing security functions with the secure encryption key. The processor is operable in a first mode wherein the secure encryption key is used for encryption operations and for test operations and in a second mode in which the secure encryption key is only used for timestamping operations. Once the processor performs a function with the secure encryption key in the second mode it is precluded from performing further functions in the first mode with the secure encryption key. When the processor receives a first request to perform a timestamping operation on first digital data while in the first mode of operation, the processor is automatically placed in the second mode of operation. After the processor has been placed in the second mode of operation a unique code for being embedded within timestamped digital data is provided; for example, the unique code is generated based on the private key and the time when the operation is requested. Therefore, the unique code is indeterminable before receipt of the first request.

[0033] Alternatively, the unique code is generated before receipt of the first request and stored within a secure module only accessible by the processor.

[0034] Data indicative of a real time value of the first request for a timestamping operation is then provided to the processor from a real time clock, shown in Fig. 2b. Based on the data indicative of a real time value, a first timestamp is generated using the real time value. The first timestamp is embedded within the first digital data, a portion thereof, or a hash thereof and the unique code is inserted within the first digital data. The first digital data with the inserted data therein are then encoded to form timestamped digital data.

[0035] Optionally, the step of encoding the first digital data includes the step of encrypting the digital data with the secure encryption key.

[0036] Referring to Fig. 2c a simplified flow diagram of a secure timestamping operation according to the invention is shown. Here, a second request to perform a timestamping operation on second digital data is received. Therefore, the processor is now in the second mode of operation after receipt of the first request, shown in Figs. 2a and 2b. Data indicative of a real time value of the second request for a timestamping operation are provided to the processor from the real time clock. Based on the data indicative of the real time value a second timestamp is generated. The second timestamp is embedded within the second digital data and the unique code is inserted within the second digital data. The second digital data with the inserted data therein are then encoded using the encryption key to form timestamped digital data.

[0037] Other embodiments of a method for securely timestamping digital data according to the invention are illustrated in the simplified flow diagrams of Figs. 3a - 3d. Here, the processor is placed in the second mode of operation before receipt of a first request to perform a timestamping operation as shown in Fig. 3a, for example, by setting a flag indicating a time instance for placing the processor in the second mode. After the processor is placed in the second mode of operation the unique code for being embedded within timestamped digital data is generated and/or provided.

[0038] Referring to Fig. 3b a method for securely timestamping digital data according to the invention is shown. A request to perform a timestamping operation on digital data is received. Data indicative of a real time value of the request for a timestamping operation is provided from a real time clock. A timestamp based on the data indicative of the real time value is generated. The digital data are then timestamped by embedding the timestamp within the digital data. In the last step the unique code is inserted within the data which is then encoded to form a timestamp.

[0039] Referring to Fig. 3c another method for securely timestamping digital data according to the invention is shown. A request to perform a timestamping operation on digital data is received. Data indicative of a real time value based on a time of the request for a timestamping operation from a real time clock. The digital data are then hashed and after inserting the unique code the hashed digital data are encrypted with the data indicative of the real time using the secure encryption key.

[0040] Fig. 4 illustrates a simplified flow diagram of the processing of securely timestamped digital data according to the invention. Upon receipt of the securely timestamped digital data the timestamp is decrypted using a key corresponding to the secure encryption key for providing time data in dependence thereupon. In the following step the unique code is retrieved from the securely timestamped digital data. The unique code is then compared with reference data in order to produce a comparison result, and if the comparison result is indicative of a match authenticity of the time data is indicated. This process of verifying the time data is essentially same for timestamped digital data provided by using the various embodiments according to the invention disclosed above. As is evident to persons of skill in the art, there are numerous methods to provide the reference data for verifying the time data. For example, the timestamping module or a timestamping authority provides the reference data to a recipient of the timestamped digital data where the data are processed to produce a comparison result. Alternatively, the recipient transmits the retrieved unique code to the timestamping authority for verification.

[0041] Referring to Fig. 5 a secure system 100 for securely timestamping digital data according to the invention is shown. The system 100 comprises at least a port 102 for receiving the digital data and for providing the timestamped digital data. The timestamping operation is

performed using a processor 104. The processor is operable in a first mode wherein a secure encryption key is used for encryption operations and for test operations and in a second mode in which the secure encryption key is only used for timestamping operations. Once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions with the secure encryption key in the first mode. During the timestamping operation in the second mode the processor 104 inserts a unique code within the timestamped digital data. The unique code is indeterminable outside the system before the processor is placed in the second mode. The unique code is generated by the processor 104 or, alternatively, received from another processor when placed in the second mode. The system 100 further comprises a real time clock 106 for providing data indicative of a real time.

[0042] Optionally, the processor 104 further comprises circuitry 108 for generating a secure encryption key. Further optionally, the processor 104 comprises circuitry 110 for generating a random number.

[0043] Further optionally, the system 100 comprises secure memory for storing the secure encryption key inaccessible outside of the secure system but accessible to the processor for performing security functions therewith.

[0044] The methods and system for securely timestamping digital data according to the invention overcomes the drawbacks of the prior art by providing means to a recipient of timestamped data to reliably verify the authenticity of same as shown above, thus rendering attempts to tamper timestamps futile. The invention provides means for reliably establishing the date of any electronic document such as digital representations of readable text but also of video, audio, and pictorial data increasing security for the exchange of digital data between parties of a transaction. Therefore, with the increasing use of the Internet for numerous business transactions secure timestamping of digital data is essential to establish credibility in such transactions.

[0045] Numerous other embodiments of the invention will be apparent to persons skilled in the art without departing from the spirit and scope of the invention as defined in the appended claims.